

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 3, 5-7, 9, 11-13, 15, 16 and 18-20 are pending in the present application. Claims 1, 7 and 19 are amended; and Claims 4 and 10 are canceled by the present amendment. Support for the amended claims can be found in the original specification, claims and drawings.¹ No new matter is added.

In the Final Office Action of March 20, 2008 (herein, the Final Office Action), Claims 1, 3-7, 9-13, 15, 16 and 18-20 were rejected under 35 U.S.C. § 103(a) as unpatentable over Timmer (U.S. Pub. 2002/0107895) in view of Shurts (U.S. Pat. 5,572,673).

Applicant respectfully traverses this rejection as independent Claims 1, 7, 13, 16, 19 and 20 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1, for example, recites a mobile information communication device, comprising:

... a central control unit which ...stores metadata received through said wireless communication unit in a corresponding partition of the metadata storage unit based on matching the received metadata with a security level and/or category predetermined by the user, and ***sets a higher security level for data received through a relatively secure communication path and a lower security level for other received data...***

Independent Claims 7, and 19, while directed to alternative embodiments, are amended to recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1, 7 and 19.

As noted above, independent Claims 1, 7 and 19 are amended to incorporate the subject matter of dependent Claims 4 and 10, but are clarified to recite that the central control unit of the mobile information communication device sets a higher security level for data

¹ Claims 1, 7 and 19 are amended to incorporate the subject matter of canceled Claims 4 and 10, and are further amended to clarify that a higher security level is set for data "received" through a more secure communication path. Support for this feature can further be found at pp. 17-18 of the specification.

received through a relatively secure communication path and a lower security level for other *received* data.

In rejecting Claims 4 and 10, the Final Office Action relied on col. 1, l. 53 – col. 2, l. 5 of Shurts noting that “the more sensitive data gets a higher level or category... the more sensitive data is typically transmitted in the more secured transmission system.” However, the cited portion of Shurts fails to disclose any sort of configuration in which a plurality of transmission system are used to receive data, much less that the system “*sets a higher security level for data received through a relatively secure communication path and a lower security level for other received data...*,” as recited in amended independent Claim 1.

More particularly, col. 1, l. 53 – col. 2, l. 5 of Shurts describes that a security policy, known as "mandatory access control" or MAC, gives "subjects" access to database objects on the basis of sensitivity labels only. A subject is an active entity, such as a user at a workstation or a command that acts on behalf of the user. An object is a passive entity that contains or receives information. Examples of objects include database tables, rows, views, and procedures. Before any object is accessed in a MAC system, the subject's sensitivity label is compared with the object's sensitivity label to determine whether the subject is allowed to access the object in the manner requested. If this comparison shows that the subject does not have a clearance dominating that of the object, read access is denied. Also, if the comparison shows that the object does not have a label dominating that of the subject, write access is denied.

Thus, the cited portion of Shurts merely describes that a subject's sensitivity level is compared against a sensitivity level of an object being accessed in order to determine whether the subject may have a label that dominates the object. Shurts, therefore, does not describe that the object receives data via a plurality of communication paths having different security levels, whatsoever. Instead, Shurts merely describes that the ability of a user at a

workstation, or a command that acts on behalf of the user, to access an object, is defined based on a relationship between the sensitivity level of the subject and the sensitivity level of the object. Shurts, therefore, fails to teach or suggest “*set[ing] a higher security level for data received through a relatively secure communication path and a lower security level for other received data...*,” as recited in amended independent Claim 1.

Further, as noted above, p. 9 of the Final Office Action asserts that “... more sensitive data is typically transmitted in the more secured transmission system.” However, as the Final Office Action fails to cite any support or provide any rationale for this assertion, Applicant respectfully traverses this assertion.

Nonetheless, even if more sensitive data is transmitted via a more secure system, Shurts fails to teach or suggest that the security level for data is set based on the transmission system via which the data is received. Instead, if more sensitive data is transmitted over a more secure transmission system, then the sensitivity level of the data is known in advance because the subject (e.g., a user at a workstation, or a command that acts on behalf of the user) must first be authorized to access the object. Thus, the sensitivity level of the data is defined by the data itself, and would not be based on the communication path via which the data is transmitted.

Further, Timmer describes a method for creating a personalized book including content of a user’s choice, such as streaming video and interactive content, in a structure designed by the user.² Timmer, however, also fails to teach or suggest that a security level of data is set in accordance with the security of a communication path via which data is received.

Therefore, Shurts and Timmer, neither alone, nor in combination, teach or suggest a mobile information communication device that includes “a central control unit which ... *sets a*

² Timmer, Abstract.

higher security level for data received through a relatively secure communication path and a lower security level for other received data...,” as recited in amended independent Claim 1.

Accordingly, Applicant respectfully request that the rejection of Claim 1 (and the claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn. For substantially similar reasons, it is also submitted that independent Claims 7 and 19 also patentably define over Timmer and Shurts.

Regarding independent Claims 13, 16 and 20, Claim 13, for example, recites an information exchange and human relation fostering support system for supporting information exchange and fostering of human relations between a plurality of users in the virtual world, comprising:

...at least one stationary communication device configured to acquire metadata from each mobile information communication device via a wireless transmission, ***compare the acquired metadata and display the result of the comparison.***

Independent Claims 16 and 20, while directed to alternative embodiments, recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 13, 16 and 20.

In rejecting independent Claims 13, 16 and 20, the Final Office Action asserts that these claims “are substantially the same as claims 1-6 above...” This, however, is simply not the case. Independent Claim 1, for example, is directed to a mobile information communication device that stores metadata log information, while Claim 13 is directed to a system including a stationary communication device that is configured to “acquire metadata from each mobile information communication device via a wireless transmission, ***compare the acquired metadata and display the result of the comparison.***”

The Final Office Action fails to address the above noted claim feature, and Applicant respectfully submits that Timmer and Shurts, neither alone, nor in combination, teach or

suggest a stationary communication device the acquires and compared metadata, as required by independent Claims 13, 16 and 20.

Accordingly, Applicant respectfully requests that the rejection of Claims 13, 16 and 20 (and any claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn.

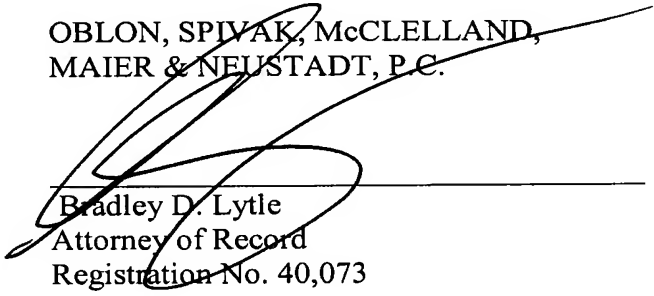
Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3, 5-7, 9, 11-13, 15, 16 and 18-20 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959